Note $\mathbb{Q}(\sqrt{3}, \sqrt{6}) = \mathbb{Q}(\sqrt{3}, \sqrt{2})$ (let $a=2$) (Hint on #66)

↑ to Day 4

Another important example of an automorphism:

Let F be a finite field, say of order p^n (p prime, $n \geq 1$).

The Frobenius automorphism $\sigma_p : F \to F$ is defined by $\sigma_p(a) = a^p$.

Why is this an automorphism?

F has characteristic $p \Rightarrow (a+b)^p = a^p + b^p$ ✓

$(ab)^p = a^p b^p$ ✓

homomorphism ✓

Note $\ker(\sigma_p) = \{a \in F : \sigma_p(a) = 0\}$

$= \{a \in F : a^p = 0\} = \{0\}$

↑ I. Domain.

$\Rightarrow \sigma_p$ is 1-1, $|F|$ is finite $\Rightarrow \sigma_p$ is onto

$\Rightarrow \sigma_p$ is an automorphism.

Note $F_{\{\sigma_p\}} \cong \mathbb{Z}_p$.

{ Suppose $\sigma_p(a) = a$ for some $a \in F$

$\Rightarrow a^p - a = 0$.

This is satisfied by $a = 1, 1+1, 1+1+1, \ldots$ $\underbrace{1+1+\cdots+1}_{=0 \text{ if } p \text{ finite}}$

But $x^p - x$ has distinct roots,

since $f'(x) = px^{p-1} - 1 = -1 \neq 0$.)

No other element satisfies $a^p - a = 0$)

$\Rightarrow F_{\{\sigma_p\}} = \{0, 1, 1+1, \ldots, \underbrace{1+1+\cdots+1}_{p-1}\} \cong \mathbb{Z}_p$.

Isomorphism Extension Theorem

Let E be an alg. extension of a field F, and let $\sigma : F \to F'$ be an isomorphism. Then σ can be extended to an isomorphism $\tau : E \to E'$, where $F' \leq E' \leq \overline{F'}$, such that $\tau(a) = \sigma(a)$ $\forall a \in F$.

Idea of Proof: any such τ has to take roots of polys. to roots of an equivalent polynomial. Can extend to $F(\alpha) \to F'(\tilde{\alpha})$. Keep on going - use infinite induction (Zorn's Lemma)

Cor: Let $\overline{F}$ and $\overline{F}'$ be any two algebraic closures of F. Then $\overline{F} \cong \overline{F}'$.

Pf: Extend the identity map to get $\sigma : \overline{F} \to \overline{F}'$. Similar extend identity map to get $\tilde{\sigma} : \overline{F}' \to \overline{F}$. ☐

Cor: Let $E \subseteq F$ be an alg. ext. of F. Sp, $\alpha, \beta \in E$ are conjugate over F. Then $\psi_{\alpha,\beta} : F(\alpha) \to F(\beta)$ can be extended to $\widetilde{\psi}_{\alpha,\beta} : E \to E' \leq \overline{F}$.

Thm: Let E be a finite-dim'l algebraic extension of F, and let $\sigma : F \to F' \leq \overline{F'}$ be an isomorphism. Then the number of extensions $\tau : E \to E' \leq \overline{F'}$ is finite,

and the number of extensions $\{E:F\}$ only depends on E, F (not on σ, F', E', F, F').

(index of E over F)

Idea of proof: Given an irreducible polynomial $f(x)$ that $\alpha \in E$ satisfies, there are only a finite # of other roots of α that α can be mapped to via τ — roots of $\sigma(f(x))$ as a polynomial over F'!

$F(\alpha)$ is a subfield of E, $[F(\alpha):F] > 1$,

so $[E:F(\alpha)] < [E:F]$

Keep going with different roots $\beta, \dots$

until $E = F(\alpha, \beta, \dots, \gamma)$ ← This has a finite # of extensions of σ (multiple of # roots)...

Corollary of this fact

If F, E, K are fields, $F \subseteq E \subseteq K$,

then $\{K:F\} = \{K:E\}\{E:F\}$.

(Similar to tower thm)

Galois Extensions of Fields.

If F is a field, and E is an algebraic extension field, then E is called a Galois extension if

(1) E is normal.

(2) E is separable.

An extension field E of the field F is normal if it is the splitting field of a set of polynomials.

eg $\bar{F}$ is normal (splitting field of the set of all polynomials).

eg. $\mathbb{Q}(\sqrt{2})$ is normal, because $\mathbb{Q}(\sqrt{2})$ is the splitting field of x^2-2.

eg. $\mathbb{Q}(2^{1/4})$ is not normal, because

$$\text{irr}(2^{1/4}, \mathbb{Q}) = x^4 - 2$$
$$= (x^2-\sqrt{2})(x^2+\sqrt{2})$$
$$= (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x+i\sqrt[4]{2})(x-i\sqrt[4]{2})$$

Splitting field of x^4-2 is $\mathbb{Q}(2^{1/4}, i)$.

$$\left[i \cdot \frac{1}{2}(\sqrt[4]{2})^3 \cdot (i\sqrt{2}) = \frac{2}{2} i = i \right] \checkmark$$

eg. $\mathbb{Q}(\sqrt{2}, \sqrt{5})$ is normal because it is the splitting field of x^2-2, x^2-5.